UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,477	07/14/2004	James E. Aston	014682.000010	4476

44870 7590 07/27/2009

MOORE & VAN ALLEN, PLLC For IBM
P.O. Box 13706
Research Triangle Park, NC 27709

EXAMINER	
DWIVEDI, MAHESH H	
ART UNIT	PAPER NUMBER
2168	

MAIL DATE	DELIVERY MODE
07/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents

United States Patent and Trademark Office

P.O. Box 1450

Alexandria, VA 22313-1450

www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS

AND INTERFERENCES

Application Number: 10/710,477

Filing Date: July 14, 2004

Appellant(s): ASTON ET AL.

Charles L. Moore

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/13/2009 appealing from the Office action mailed 11/16/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0194490	Halperin et al.	12/19/2002
2004/0025015	Satterlee et al.	02/05/2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-2, 5, 7-9, and 12-19 are rejected under 35 U.S.C. 102(b) as being anticipated by **Halperin et al.** (U.S. PGPUB 2002/0194490).

3. Regarding claim 1, **Halperin** teaches a method comprising:

A) flagging a program on a computer as being suspect for possibly containing a virus in response to at least one of: opening a local file on a local file system of the computer to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system and at least the medium security level being set (Abstract, Paragraphs 73-77, and 88-108);

B) storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program (Paragraphs 108).

The examiner notes that **Halperin** teaches **"flagging a program on a computer as being suspect for possibly containing a virus in response to at least one of: opening a local file on a local file system of the computer to perform a read operation and opening a shared file on a shared or network file system to perform**

a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system and at least the medium security level being set" as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers…Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment

actions such as, but not limited to:… Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77). The examiner further notes that **Halperin** teaches **"storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 2, **Halperin** further teach a method comprising:

A) inhibiting a write or append operation associated with program in response to flagging the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"inhibiting a write or append operation associated with program in response to flagging the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination

is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 5, **Halperin** further teaches a method comprising:

A) sending an alert in response to flagging the program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to flagging the program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:…Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 7, **Halperin** further teaches a method comprising:

A) sending an alert to a network monitoring system in response to flagging the program (Paragraph 111).

The examiner notes that **Halperin** teaches **"sending an alert to a network monitoring system in response to flagging the program"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 8, **Halperin** further teaches a method comprising:

A) logging any file system operations including recording a filename and a location where the local or shared file is written (Paragraph 108).

The examiner notes that **Halperin** teaches **"logging any file system operations including recording a filename and a location where the local or shared file is written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose

destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 9, **Halperin** teaches a method comprising:

A) allowing a security level to be set (Paragraphs 43-44, 108, and 111);

B) monitoring predetermined file system operations associated with a program (Abstract, Paragraphs 73-77, and 88-108); and

C) logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written (Paragraphs 108).

The examiner notes that **Halperin** teaches **"allowing a security level to be set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file

types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"monitoring predetermined file system operations associated with a program"** "Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include…Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and " Any known

behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers…A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that **Halperin** teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g.,

only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 12, **Halperin** further teaches a method comprising:

A) receiving a notification that the program intends to perform one of the predetermined file system operations (Paragraph 108).

The examiner notes that **Halperin** teaches **"receiving a notification that the program intends to perform one of the predetermined file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have

attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 13, **Halperin** further teaches a method comprising:

A) following a predefined procedure in response to the level of security set (Paragraphs 43-44, 108, and 111).

The examiner notes that **Halperin** teaches **"following a predefined procedure in response to the level of security set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific

types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 14, **Halperin** further teaches a method comprising:

A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal

operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers…Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:… Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 15, **Halperin** further teaches a method comprising:

A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any

content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated

target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers…Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:… Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 16, **Halperin** further teach a method comprising:

A) inhibiting any predetermined file system operations associated with program in response to the program being flagged (Paragraph 108).

The examiner notes that **Halperin** teaches **"inhibiting any predetermined file system operations associated with program in response to the program being flagged"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may

also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 17, **Halperin** further teaches a method comprising:

A) sending an alert in response to the program attempting to perform any predetermined file system operations (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to the program attempting to perform any predetermined file system operations"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:…Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 18, **Halperin** further teaches a method comprising:

A) sending the alert to a network monitoring system (Paragraph 111).

The examiner notes that **Halperin** teaches **"sending the alert to a network monitoring system"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 19, **Halperin** further teaches a method comprising:

A) presenting an alert to a user for approval before the predetermined file system operation is performed by the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"presenting an alert to a user for approval before the predetermined file system operation is performed by the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent

by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 3-4, 10-11, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Halperin et al.** (U.S. PGPUB 2002/0194490) as applied to claims 1-2, 5, 7-9, and 12-19, in view of **Satterlee et al.** (U.S. PGPUB 2004/0025015).

6. Regarding claim 3, **Halperin** does not explicitly teach a method comprising:

A) monitoring all file operations associated with the program in response to the program not being in a safe list.

Satterlee, however, teaches **"monitoring all file operations associated with the program in response to the program not being in a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 4, **Halperin** does not explicitly teach a method comprising:
A) permitting selected read and write operations in response to a predefined rules table.

Satterlee, however, teaches **"permitting selected read and write operations in response to a predefined rules table"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a

predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 10, **Halperin** does not explicitly teach a method comprising:
A) selecting a program for monitoring in response to the program not being on a safe list.

Satterlee, however, teaches **"selecting a program for monitoring in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 11, **Halperin** further teaches a method comprising:

A) logging any file system operations (Paragraph 108).

The examiner further notes that **Halperin** teaches **"logging any file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file

types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Halperin does not explicitly teach:

A) associated with any programs on the safe list.

Satterlee, however, teaches **"associated with any programs on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 20, **Halperin** further teaches a method comprising:

A) requiring approval before performing any predetermined file system operations associated with the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"requiring approval before performing any predetermined file system operations associated with the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Halperin does not explicitly teach:

A) in response to the program not being on a safe list.

Satterlee, however, teaches **"in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but

other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

(10) Response to Argument

A. Claims 1-2, 5, 7-9, and 12-19 are rejected under 35 U.S.C. 102(b) as being anticipated by **Halperin et al.** (U.S. PGPUB 2002/0194490).

1. Independent Claim 1

Arguments (1): Regarding Independent Claim 1, Appellant argues that "The Final Office Action dated as mailed November 16, 207, cited the Abstract, Paragraphs 73-77, and 88-108 of Halperin in rejecting these features of Claim 1. The Abstract of Halperin recites…Accordingly, from the abstract of Halperin, Halperin teaches detection of malicious software in a plurality of computing devices within a network and not within an individual computer as provided by the present invention. Halperin does not teach or suggest flagging a program on a computer as being suspect for possibly containing a virus, nor Halperin teach or suggest the specific conditions associated with the computer for flagging the program on the computer as provided by the embodiment of the present invention as recited in Claim 1".

However, the examiner wishes to refer to the Abstract of Halperin which states "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract). The examiner further wishes to state that grouping computing devices into a consortium that is suspected of malicious activity clearly shows that the scope of Halperin is directed towards virus detection (exactly of what the scope of the instant invention is directed towards). Moreover, all of the cited portions of Halperin clearly show that there is detections of virus activity within a computer.

Arguments (2): Regarding Independent Claim 1, Appellant argues that "Paragraphs 73-77 of Halperin, also cited in the Final Office Action in rejecting Claim 1…Halperin teaches suspending messages being sent by an infected computer but Halperin does not teach or suggest flagging a program on the computer based on specific local file system operations as provided by the embodiment of the present invention as recited in Claim 1 of the present application".

However, the examiner wishes to state that only one of the four local specific file system operations is required to be taught by **Halperin** due to the "at least one of" language of the independent claims. Moreover, the examiner wishes to refer to paragraphs 73 of **Halperin** which states that "As the virus attempts to propagate it selects one or more valid and decoy addresses from address book 102 and folders 104, automatically generates messages that incorporate the virus, typically as an

attachment, and forwards the messages to server 108" (Paragraph 73). The examiner further wishes to state that the limitation "the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system" is taught by the aforementioned citation of **Halperin**. Specifically, the virus of **Halperin** manipulates an email application by reading or opening itself up by being functionally active in performing malicious activity. Moreover, by attaching a copy of itself in an e-mail message, the virus teaches writing or appending any content to the local file on the local file system.

Arguments (3): Regarding Independent Claim 1, Appellant argues that "Applicant further respectfully submits that there is no teaching or suggestion in Halperin of the specific local file system operations being performed on the computer for determining whether to flag a program on the computer as being suspect for possibly containing a virus. Halperin merely teaches initiating virus scanning and virus containment actions associated with email messages at the server and network level as opposed to the file system operations at the computer level or client level as required by the embodiment of the present invention as recited in Claim 1".

However, the examiner wishes to state that only one of the four local specific file system operations is required to be taught by **Halperin** due to the "at least one of" language of the independent claims. Moreover, the examiner wishes to refer to paragraphs 73 and 76-77 of **Halperin** which state that "As the virus attempts to propagate it selects one or more valid and decoy addresses from address book 102 and

folders 104, automatically generates messages that incorporate the virus, typically as an attachment, and forwards the messages to server 108" (Paragraph 73) and "Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 76-77). The examiner further wishes to state that the limitation "the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system" is taught by the aforementioned citation of **Halperin**. Specifically, the virus of **Halperin** manipulates an email application by reading or opening itself up by being functionally active in performing malicious activity. Moreover, by attaching a copy of itself in an e-mail message, the virus teaches writing or appending any content to the local file on the local file system. In addition, by scanning for actions done by the potential virus at computer 100 and notifying a user of computer 100 of such actions, then as a result, Halperin clearly teaches monitoring local actions at a specific computer (computer 100).

Arguments (4): Regarding Independent Claim 1, Appellant argues that "The Final Office Action also cited paragraphs [0088]-[0108] in rejecting the specific file system operations as recited above in Claim 1. Paragraphs [0088]-[0096] describe specific target behavior profiles and provides a list of examples. Applicant respectfully submits that paragraphs [0088]-[0096] of Halperin also do not teach or suggest the specific local file system operations being performed on the computer for determining

whether to flag a program on the computer as being suspect for possibly containing a virus as recited in Claim1".

However, the examiner wishes to state that paragraphs 73-77 were uses to specifically teach the claimed local file system operations. Paragraphs 88-96 were used to teach the claimed flagging of potential virus programs at specific computers.

Arguments (5): Regarding Independent Claim 1, Appellant argues that "Paragraphs [0097] of Halperin beginning at line 6…Applicant respectfully submits that there is no teaching or suggestion in Halperin of flagging a program on an individual computer as being suspect for possibly containing a virus".

However, the examiner wishes to refer to Paragraphs 97-107 of Halperin which state "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers…Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107). The examiner further wishes to state, in contrast to appellants unfounded assertions, that Halperin clearly teaches flagging potential infected programs at specific computers (See "an

indication that a computer virus may have infected ***those computers***"). Specifically, Halperin teaches using patterns to see if specific individual computers 500 have been infected with viruses.

Arguments (6): Regarding Independent Claim 1, Appellant argues that "Applicant respectfully submits that none of the suspicious behavior patterns taught by Halperin teach or suggest the specific conditions or file system operations recited in Claim1 for flagging the program on the individual computer".

However, the examiner wishes to state that paragraphs 73-77 were uses to specifically teach the claimed local file system operations. Paragraphs 97-107 were used to teach the claimed flagging of potential virus programs at specific computers.

Arguments (7): Regarding Independent Claim 1, Appellant argues that "Applicant respectfully submits that Halperin teaches away from the present invention in that Halperin quarantines the messages and does not allow them to reach their intended destinations. In contract, the present invention, as recited in the embodiment of Claim 1, permits the file to be copied or written by the program at its intended location and then stores the file name and location where the local or shared file is copied or written".

However, the Applicants are also reminded that in order to disqualify a reference based on a "teach away" reasoning, the reference has to *explicitly* suggest or disclose the so-called teach away steps - Applicants assertion can not be accepted if it is unsupported by a valid evidence. In this case, Halperin does teach the writing of the e-mail message by the virus that, as a result, teaches the operations recited in the

independent claims. Moreover, because Halperin teaches the recognition of the decoy address and the notification of the user of the specific computer of a potential virus, Halperin teaches the location of where the e-mail was written and where it was intended to be sent. Furthermore, by quarantining the entire e-mail message (including attachments), Halperin teaches storing the filename of the message.

Arguments (8): Regarding Independent Claim 1, Appellant argues that "In further distinction, Halperin teaches storing an entire message, not only a name or identification as in the present invention. The message in Halperin is not allowed to be sent to its intended destination. Accordingly, there is no need for Halperin to store a file name and a location where the file is copied or written as in the present invention".

However, in contrast to appellants unfounded assertions, the examiner wishes to state that Halperin allows stored messages to be sent to their intended destination after user review (See "may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108)). Moreover, appellants assertions regarding that there is no need to store filenames and locations is without merit. Specifically, Halperin teaches that messages including attachments are stored. Thus, filenames are clearly recorded in that attachments are stored. Moreover, because a sender is recorded and included in stored messages, then the location from where the message is written is recorded as well.

2. Independent Claim 9

Arguments (1): Regarding Independent claim, Appellants argue that "The Office Action cited paragraph [0108] of Halperin in rejecting this feature of Claim 9. As previously discussed, Halperin teaches in paragraph [0108] quarantining at a server messages believed to contain a virus. In contrast, the present invention as recited in Claim 9 permits the file to be written and then records the file name and the location where the file is written. As discussed above, Halperin does not teach or suggest this feature of the present invention".

However, Independent Claim 9 merely claims "logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written". The examiner further wishes to refer to Paragraph 108 of Halperin which states "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific

types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108). The examiner further wishes to state that a server storing written messages including attachments for a user to review teaches the aforementioned limitation. Specifically, the stored message includes the attachments (filename) and the sender (location). Moreover, because a sender (i.e., virus) who sends a message with attachments must first "write" that message with attachments locally, then the limitation of "in response to being written" is taught. Furthermore, because the messages are stored for user review, then their filenames are logged. In addition, because the location from with which the messages were sent is recorded, then the location where the message was written is taught as well.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Mahesh Dwivedi
Patent Examiner
AU 2168
/Mahesh H Dwivedi/
Examiner, Art Unit 2168

/Tim T. Vo/

Supervisory Patent Examiner, Art Unit 2168

/Eddie C. Lee/

Supervisory Patent Examiner, TC 2100